REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
On-Line tudományos folyóirat
XXVII. évfolyam 2015. 2. szám

Ványa László[1]

NAVIGÁCIÓS BERENDEZÉSEK ZAVARÁSA ÉS MEGTÉVESZTÉSE[2]

Az elektronikai hadviselés fontos része az elektronikai ellentevékenység, amely magába foglalja többek között az elektronikai zavarást és az elektronikai megtévesztést. A repülésben használt navigációs berendezéseket is fenyegetik a speciális eszközökkel létrehozott zavarjelek. A cikk bemutatja néhány navigációs rendszer elektronikai támadásának módszerét. A 80-as években már a TACAN harcászati rádió-navigációs rendszerre is létezett mobil zavaró állomás, de a mai korszerű globális műholdas helymeghatározó rendszereket is többféle zavarási módszer fenyegeti.

JAMMING AND DECEPTION OF NAVIGATION SYSTEMS

The electronic countermeasure is important part of electronic warfare, which consists of electronic jamming and electronic deception. The jamming signals, made by special equipment threaten the navigation systems, used in aviation. This article presents methods of electronic attack against some navigation systems. There was a mobile jamming station against tactical radio navigation system TACAN at 80s and there are several jamming methods against modern global satellite navigation systems too.

BEVEZETÉS

Az elektronikai hadviselés aktív, támadó oldalához tartozik a szemben álló fél elektronikai berendezéseinek zavarjelekkel, zavaró hatásokkal való besugárzása, amely következtében azok a rendeltetésüknek megfelelő feladatokat nem, vagy csak korlátozottan képesek ellátni. A támadó oldal általában egy lépés hátrányban van, mivel először meg kell ismernie a szemben álló fél újabb berendezésének paramétereit, működési elvét, sebezhető pontjait és csak az után kezdhet bele egy-egy speciális eljárás, berendezés kidolgozásába.

Az elmúlt évtizedekben kidolgozott elektronikai hadviselési zavaró állomások nagy része általános rendeltetésűnek mondható. Ilyenek például a rövid- és ultrarövid-hullámú rádiózavaró állomások, amelyek a teljes 1,5–30 MHz, illetve 20–100 MHz tartományt átfogták és nem egy adott rendszer ellen készültek. Ilyenek voltak a légvédelmi rádiótechnikai zavaró állomások, amelyek az adott hullámtartományban működő igen sokféle rádiólokátor ellen hatékonyan vették fel a harcot, vagy akár a rádiógyújtó zavaró állomások, amelyek a rádiógyújtóval szerelt tüzérségi lövedékek, aknagránátok zavarására készültek.

A zavaró berendezések másik csoportja speciálisan egy-egy konkrét rendszer ellen készült. Ezek működési elvüket, eljárásaikat tekintve szofisztikáltabbak voltak, általában nem működésképtelenné tették a szemben álló fél berendezését, hanem célszerűen észrevétlenül meghamisították annak mérését, átvették felette az irányítást, majd a valóságtól egyre inkább eltávolodó információtartalmú jelekkel eltérítették eredeti feladatától. A szárazföldi tájékozódásban

[1] ezredes, habilitált egyetemi docens, Nemzeti Közszolgálati Egyetem, HHK, vanya.laszlo@uni-nke.hu
[2] Lektorálta: Prof. Dr. Makkay Imre ny. ezredes, egyetemi tanár, drmi48@gmail.com

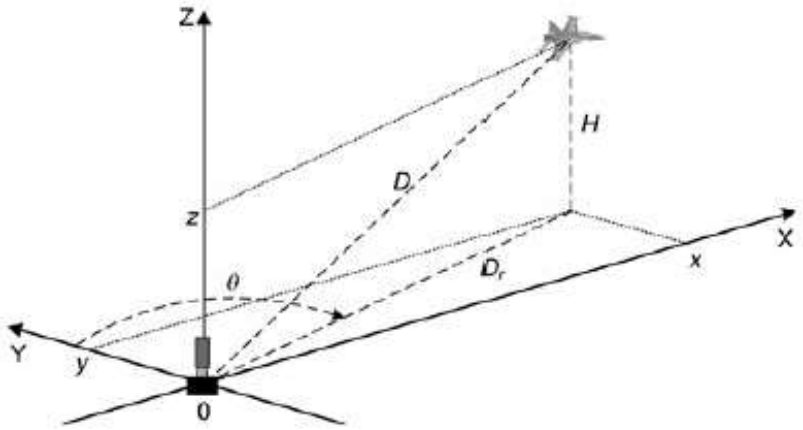
és a repülésben használatos, elsősorban rádiótechnikai elvű navigációs berendezések is évtizedek óta célobjektumai az elektronikai hadviselésnek.

Az elektronikai zavarás és a megtévesztés a gyakorlatban nem egy és ugyanaz. A 2. kiadású Összhaderőnemi Elektronikai Hadviselés Doktrína definíciója szerint: *„Az elektronikai zavarás az elektronikai ellentevékenységi funkció azon része, amely az elektromágneses energia szándékos kisugárzásával, visszasugárzásával vagy visszatükrözésével megakadályozza vagy korlátozza az ellenség által használt elektronikai eszközök, berendezések és rendszerek alkalmazását.”* … *„Az elektronikai megtévesztés az elektronikai ellentevékenységi funkció azon része, amely az elektromágneses energia szándékos kisugárzásával, visszasugárzásával, módosításával, elnyelésével vagy visszatükrözésével biztosítja az ellenség vagy annak elektronikai rendszereinek megzavarását, félrevezetését vagy akadályozását.”* [1] A két meghatározás között árnyalatnyi különbség van, de az a gyakorlati alkalmazás szempontjából igen jelentős lehet. Az elektronikai zavarással okozott rendeltetés szerinti működés akadályozása általában nyilvánvalóvá válik a kezelő számára, amíg a szakszerűen kivitelezett megtévesztés hatása észrevétlen, de a berendezés valótlan adatokat, célokat, paramétereket, helyzeteket szolgáltat. Egy kézenfekvő példa: ha a repülőgép vezető rádióösszeköttetését rendszeresen jellegzetes szaggatások, hanghatások akadályozzák, akkor minden valószínűség szerint szándékos zavaró tevékenységgel áll szemben. Ha azonban a légi irányítás jól ismert hangján más parancsok érkeznek, akkor ez teljesen hihető lehet, megtévesztik a végrehajtót, eltérítik az eredeti feladatától.

Jelen cikk bemutat egy olyan viszonylag réginek mondható rendszert és a speciálisan ellene kidolgozott zavaró berendezést, amely jól példázza, hogy a szofisztikált zavarási eljárás hogyan képes megoldani az észrevétlen jelátvételt és biztosítani a megtévesztés eredményességét. A cikk további részében a mai, korszerű viszonyok között széles körben használatos, globális műholdas helymeghatározó rendszer, pl. a Navstar GPS támadásának módjairól lesz szó, annak is előbb a „nyers erő” módszeréről, majd a napjainkban egyre szélesebb körben emlegetett szofisztikált megtévesztési módszeréről, a GPS spoofing-ról. Ma már bizonyos, hogy a GPS spoofing éles katonai alkalmazásán is túl van a világ.

A TACAN harcászati közelnavigációs rendszer [2]

A TACAN (Tactical Air Navigation) rendszert a nyugati országok harcászati légiereje és haditengerészeti repülőgépei számára fejlesztették ki egy adott repülőtérről vagy anyahajóról a célkörzetbe való kijutás, az útvonalrepülés és a visszatérés rádiónavigációs biztosítása céljából. Rendszertechnikáját tekintve egy úgynevezett szög- és távolságmérő rendszer volt, amely a hatótávolságán belül mintegy száz repülőgép számára biztosította, hogy a földi (tengeri) irányító állomáshoz képest meghatározza az északi irányhoz (Y) mért oldalszögét (Θ) és ferdetávolságát (D). A mennyiségek értelmezése az 1. ábrán látható. Működési frekvenciatartománya a 962–1213 MHz-es deciméteres frekvenciatartományba esett, a hatótávolsága a repülési magasság függvénye volt, 1000 m-en mintegy 100 km, 10 000 m-en mintegy 370–400 km. A frekvencia raszter 126 csatorna alkalmazását tette lehetővé 1 MHz-es lépésekben.



1. ábra. A repülőgép koordinátáinak értelmezése [3]

Bármely csatornán lehetőség volt a távolság és oldalszög meghatározásán kívül egy adatközlő csatornán parancsokat és adatokat továbbítani. A rendszer egy adott csatornája két frekvencián üzemelt. A földről a repülőgépre irányuló 1–63 föld-levegő (uplink) csatornák a 962–1024 MHz tartományban, a 64-126 föld-levegő csatornák pedig az 1151-1213 MHz tartományban dolgoztak. A repülőgép fedélzeti kérdező berendezések levegő-föld irányú (downlink) frekvenciatartománya az 1–63 csatornákhoz az 1025–1087 MHz, a 64–126 csatornákhoz pedig az 1088–1150 MHz frekvenciatartományba estek. A frekvenciapárok duplex távolsága 63 MHz.

A földi állomáson az alábbi fő egységek működnek:

- a repülőgép fedélzeti kérdező berendezés jeleinek vételére szolgáló vevő;
- impulzus üzemű adó;
- a speciális forgó antennarendszer;
- energiaellátó és egyéb berendezések.

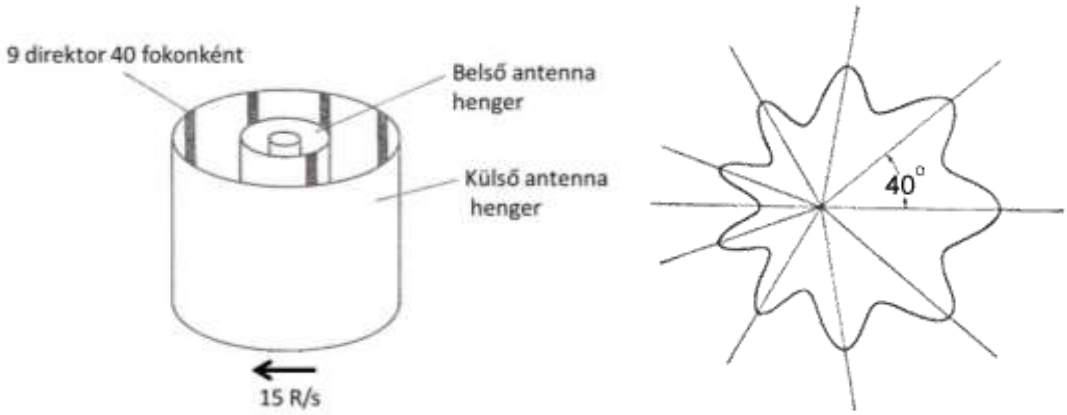
A repülőgép fedélzetén működő egységek:

- a repülőgép fedélzeti adó-vevő berendezés;
- a műszerfalra épített távolság és oldalszög indikátorok;
- az adatközlő csatorna kijelző tablója.

A távolságmérés működési elve hasonló volt az aktív rádiólokátorokéhoz, időmérésre vezették vissza. A repülőgép fedélzeti kérdező berendezés két impulzusból álló kérdezőjelet, ún. kódpárt sugároz ki. Az impulzusok szélessége 3,5 μs, közöttük 12 μs távolság van. 22–30 Hz ismétlődési frekvenciával sugározza ki az adó a követő üzemmódban. Ha a vevőkészülék elveszíti a földi állomás válaszjeleit, akkor kereső üzemmódra áll át, amikor is 120–150 impulzuspárt ad másodpercenként. A ferdetávolság mérése a repülőgép – földi állomás – jelfeldolgozás – földi állomás – repülőgép útvonalon eltelt idő mérésével történik, és folyamatosan kijelzésre kerül a pilóta számára. A távolságmérés pontossága 180 m ± 15%.

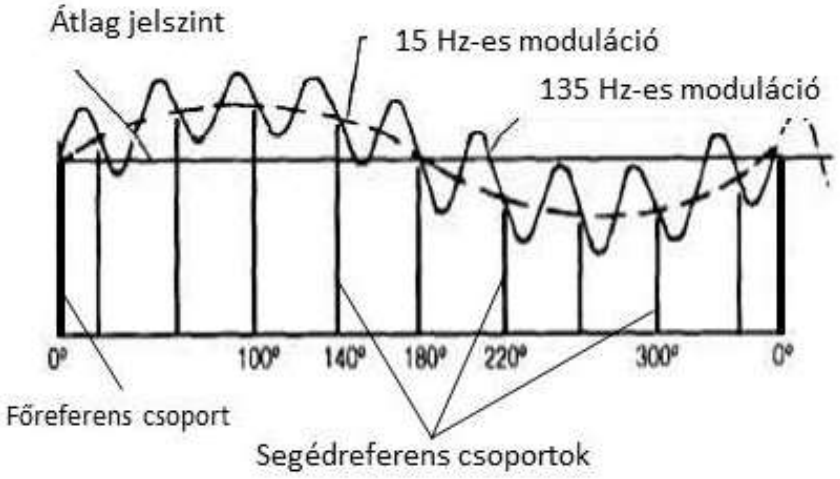
Az oldalszög meghatározása ennél jóval bonyolultabb. Az oldalszögmérő csatorna működéséhez mintegy 3000 impulzus pár/s kisugárzása szükséges a földi állomásról. Ha nincsenek a levegőben kérdező berendezések elégséges számban, akkor zajjal modulált kitöltő impulzusokat kell kisugározni.

Az oldalszög méréséhez speciális, forgó antennarendszert alakítottak ki a földi állomáson. Egy központi sugárzó körül két koncentrikus henger található, amelyek alkotója mentén helyezték el a reflektor elemeket. A belső hengeren egy, a külső hengeren kilenc darab, 40 fokonként elhelyezett reflektor modulálja amplitúdóban az eredetileg körsugárzó karakterisztikát. A hengerek 15 fordulat/s sebességgel forognak, ami a kisugárzott impulzusoknak egy 15 Hz-es és ezen belül egy 135 Hz-es burkolójú amplitúdómodulációt okoznak. (2. ábra)



2. ábra. A TACAN rendszer antennájának felépítése és poláris iránydiagramja [4][5]

Az oldalszögmérés referenciairányát a karakterisztika maximum irányának éppen keleti irányba való fordulásakor egy ún. fő referenscsoport impulzussorozat jelöli ki. Ez a fő referenscsoport 12 impulzuspárt tartalmaz, az impulzuspárok között 30 μs időtartammal. Ettől a ponttól kezdődik az oldalszög mérés a fedélzeten. Az antennarendszer a forgásakor 40 fokonként 6 impulzuspárból álló segédreferens csoportokat is kisugároz, amelyek között 24 μs idő van. Az antennarendszer által kisugárzott távolság és oldalszög információt is hordozó jel struktúrája a 3. ábrán látható.



3. ábra. A TACAN rendszer oldalszög információjának kialakítása [6]

A repülőgép fedélzetén, az iránymeghatározás durván a fő referenscsoport és a 15 Hz-es burkolójel maximuma közötti fázisméréssel határozták meg, az oldalszög pontos értékét pedig a segédreferens és a 135 Hz-es burkoló maximuma közötti fázismérés határozta meg. A repülőgépnek a földi állomáshoz viszonyított oldalszögét a pilóta számára egy műszer folyamatosan kijelezte. A mérés pontossága a fenti módszerrel elérte az 1 fokot.

Az adatcsatorna működése során a parancs és az erre adandó válasz kódolva került kisugárzásra. A repülőgép fedélzeti üzenet mintegy 3 μs időtartamú és a távolsági kérdező jelek között kerül kisugárzásra, a földi állomás adatjelét 12 μs hosszúságban, minden harmadik segédreferens csoport után adták. A földi állomások az azonosítás kedvéért 775 s-onként három karakterből álló, Morse-kódot is kisugároztak.

Az orosz gyártmányú R-388, a TACAN harcászati közelnavigációs rendszer zavaró állomása [2]

Az R-388 típusú zavaró állomás olyan földi, mozgó, automatizált berendezés, amely a TACAN rendszerbe tartozó fedélzeti vevőkészülékek oldalszög-, távolságmérő és adatközlő csatornájának zavarására készült. Egy R-388 állomás képe látható a 4. ábrán.

4. ábra. Az R-388 (NATO kód: STOVE PIPE) zavaró állomás telepített antennával. [7]

Az állomás vevőberendezése a repülőgépek fedélzeti kérdező berendezéseinek sávjában, az 1025–1150 MHz tartományban üzemel. A kérdező jelek észlelésekor azonosítja azokat, ráhangol az adott csatornára és lehangolja az adórendszert is a megfelelő duplex adófrekvencia párra. Ez megegyezik a földi TACAN állomás adófrekvenciájával. Az amplitúdóban 15 és 135 Hz-el modulált jelek imitálása céljából 5 és 14 kW impulzusteljesítménnyel sugározza ki a zavaró jeleket. A berendezés átlagteljesítménye mintegy 250 W.

Az előállított zavaró jelek időparamétereiket tekintve csak kismértékben térhetnek el az irányító állomás által előállított jelektől. Az oldalszögmérő csatorna mérésének meghamisítása érdekében az amplitúdó moduláció és a referens impulzuscsoportok közötti fázisviszonyt kell megbontani. Az irányító állomás és a zavaró állomás referens impulzus csoportjai egyidőben jelen vannak a vevőkészülékben, ami a pontos fázismérést megakadályozza.

A távolságmérő csatorna lefogásához az irányító állomás és a zavaró állomás jeleinek időben egyszerre kellene megérkezni, ami akkor teljesülne, amikor a repülőgép egyenlő távolságra van a két állomástól. Ez a helyzet a két állomás közti egyenes felező merőleges vonalában, illetve 3 dimenzióban tekintve, a felező síkban következik be. Attól kezdve, hogy a repülőgép a felező síkhoz ér, a zavaró állomás válaszjele előbb ér a repülőgéphez, mint az irányító állomás jele.

Mivel a zavaróállomás nem ismeri pontosan a földi állomás és a repülőgép közti távolságot, ezért a távolságmérő csatorna lefogása nem egyedi válaszjelekkel, hanem válaszjel impulzuspár sorozattal történik. Ekkor a fedélzeti vevő vagy a zavaró állomástól való távolságot kezdi mutatni, vagy kereső üzemmódra kapcsolja át a fedélzeti berendezéseket.

Az adatcsatorna lefogásához a zavaró állomásnak úgy kell időzítenie a zavaró impulzusokat, hogy azok egyidőben legyenek jelen a fedélzeti adatcsatorna vevőben. Mivel nem ismert, hogy mikor indul az első parancs, ezért csak a második, és minden ez után következő parancsra tudott válaszzavart előállítani.

A fentebb leegyszerűsítve összefoglalt működési elvek megismeréséből levonható az a következtetés, hogy a valóban hatékony és eredményes megtévesztő zavarás előállítása igen csak esetleges és rövid idejű. A repülőgép vezetője a zavaró állomás energetikailag hatékony zavarási zónájába érve, illetve a két földi állomás közötti felező síktól kezdve a zavaró állomás által adott jelek feldolgozásából nyert kijelzéseket látja, amelyek rendszertelenül váltakozva hol hihető, hol nem hihető értékeket adnak, vagy akár kereső módba kapcsolják át a vevőrendszert. A parancsközlő csatorna „elhallgat”, az egész rendszer bizonytalanná válik, így navigációs okokból a feladat végrehajtása kritikussá válik. Gyakorlott és erre felkészített pilóta tudni fogja, hogy erre a berendezésre a továbbiakban nem számíthat. Ugyanakkor ez hatásában olyan, mint ha a földi állomás hatótávolságának határára ért volna. A valóban szofisztikált, megjelenésében észrevétlen, hatásában mégis eredményesen megtévesztő zavarás kidolgozására néhány évtizedet várni kellett.

A NAVSTAR és más globális műholdas navigációs rendszerek zavarása

A globális műholdas navigációs rendszerekből több is létezik, illetve áll fejlesztés alatt, úgymint az amerikai NAVSTAR GPS, az orosz GLONASS, a kínai BEIDOU, illetve COMPASS, az indiai IRNSS, a japán QZSS, valamint az EU országok együttműködésével épülő GALILEO. Jelen cikk kereteiben nem térünk ki részletes ismertetésre egyik esetében sem, mivel ennek igen széles szakirodalma van, sok korábbi publikáció foglalkozik velük. Egy szempontból, a zavartatás szempontjából fogunk megoldásokat vizsgálni.

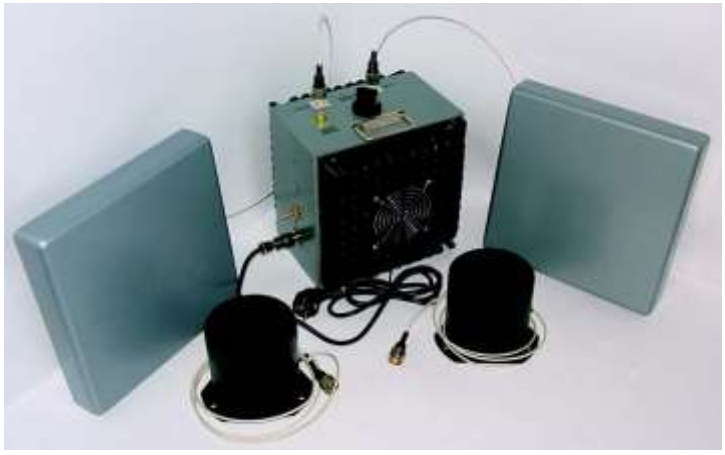
A NAVSTAR rendszer két vivőfrekvencián: L1=1575,42 MHz és L2=1227,60 MHz sugároz CDMA spektrum-kiterjesztésű kódfázis modulált jeleket. A civil vevőkészülékek csak az L1 frekvencia vételére és a C/A kód feldolgozására alkalmasak katonai megfontolásokból. A műholdak távolsága a Földtől 20200 km, ami azt jelenti, hogy a vehető jelszint igen alacsony.

A legegyszerűbb és sokáig jól is működő zavarási eljárás a jól ismert, szabványos frekvenciák célzott zajzavarása volt, amely megakadályozta a műholdak jeleinek vételét, mivel jelszintjük sok nagyságrenddel meghaladta azokat. Az 5. ábrán egy 1997. augusztus 19–24. közötti, Moszkva melletti airshow alkalmával kiállított, talán első katonai célú GPS/GLONASS zavaró berendezés képe és adatlapja látható. A 4 W kimenő teljesítménnyel 150–200 km hatásos zavarási távolságot jegyeztek, ami azt jelenti, hogy ebben a körzetben a műholdak jeleit a vevőkészülékek nem képesek feldolgozni, vagyis olyan képet mutatnak a vevők, mintha rádiófrekvenciás árnyékban lennének.

5. ábra. Egy korai orosz gyártmányú GPS/GLONASS zavaró berendezés [8]

A 6. ábrán egy GPS/GLONASS/GALILEO rendszer elleni aktív zavaró tevékenységre tervezett orosz gyártmányú zavaró berendezés látható, amelyet a 2007-es Moszkva, Zsukovszkijban megrendezett MAKS-2007 nemzetközi repülő és űrhajózási szakkiállításon állítottak ki.

6. ábra. Több műholdas navigációs rendszer ellen is alkalmas zavaró berendezés [9]



7. ábra. Az orosz Aviaconversia nagyteljesítményű GNSS zavaró berendezése [10]

A 7. ábrán látható zavaró berendezést használták a 2003-as iraki bombázások idején az amerikai JDAM (Joint Direct Attack Munition) GPS navigációval működő bombák irányítórendszerének megzavarására. Az Aviaconversia orosz haditechnikai vállalat közlése szerint a kisebb, 2–3 W kimenő hatásos teljesítményű berendezések hatótávolsága mintegy 50 km, a nagyobb, 20 W-osak hatótávolsága mintegy 150 km. [10]

A katonai célú és fejlesztésű eszközök mellett tömegével jelentek meg a webáruházakból rendelhető kisméretű, kézi zavaró berendezések, amelyek elsősorban a bűnözői körök céljait szolgálják, hiszen normális körülmények között ki másnak fűződik érdeke ahhoz, hogy meghiúsítsa a navigációs eszközök és a mobil telefonhálózat használatát. A nagy értékű gépkocsikba, teherszállító járművekbe telepített járműkövető rendszerek blokkolásával lehet alkalmat teremteni a járművek, szállítmányok ellopásához, illetve a bennük lévő jeladók hatástalanításáig. Két példa a számtalan közül látható a 8. ábrán. A kettő ára együtt 224 USD.

8. ábra. Kínai gyártmányú 3G telefon és GPS zavaró berendezések. [11]

Mindezek az eszközök és eljárások a műholdas szolgáltatás megszakításával egyértelművé teszik a kezelők számára, hogy az eredeti feladatára használhatatlan a készülékük. Az oka nem egyértelmű, de a helyzet világos.

A sztochasztikus zajzavarok ellen fejlesztették ki az ún. nullázásos (nuller) rendszerű zavarvédelmi eljárásokat. Ilyen például a NovAtel cég „GAJT™ Dual-Frequency GPS Anti-jam Antenna” nevű eszköze. [12] (9. ábra) A GAJT 7 db antennát tartalmaz, amelyek képesek 6 zavaró forrás irányba nullhelyet illeszteni az antenna iránykarakterisztikába. Az eljárás lényege, hogy minden antenna egy vezérelhető csillapító-fázistoló tagon keresztül csatlakozik a jelösszegzőre. A nagysebességű jelfeldolgozás olyan fázis és amplitúdó viszonyokat állít be, amely az adott irányban minimum, illetve nullhelyet hoz létre. [13]

Ezen kívül még jó néhány zavarvédelmi eljárás és alkalmazás létezik, (IGAS, SIRIAS, MIND, DIGAR, stb.) amelyekről pl. a [14] irodalomban lehet további információkat találni.

A továbbiakban egy olyan újnak mondható eljárás lényegét tekintjük át, amely a valóban szofisztikált, megtévesztő elektronikai zavarás módszere és ez a spoofing. Lényegét tekintve a navigációs vevőt olyan jelekkel sugározzuk be, mint ha az, egy teljesen más helyen lenne. Fő jellemzője, hogy úgy tűnik, minden teljesen rendben van, nem szakad meg a jel.

9. ábra. A GAJT (GPS Anti-Jam Technology) harcjárműre installálva [15]

A spoofing technika elsősorban a kezelő személyzet nélküli, önálló, vagy fél autonóm módon feladatot végrehajtani képes eszközök, pilóta nélküli repülőgépek, szárazföldi vagy vízi járművek, robotikai eszközök ellen jelent komoly kockázatot, de a kezelők jelenléte sem garancia arra, hogy észrevegyék a spoofing támadást.

A híradásokban több elhíresült esetet is találunk. A legnagyobb port a titkos amerikai RQ-170 lopakodó pilóta nélküli repülőgép Iránban való leszállítása verte fel 2011. december 4-én. Ezzel egy korábbi publikációm is foglalkozik.[16] Azóta a szakértők egyetértenek abban, hogy a navigációs jelek meghamisítása, vagyis a GPS spoofing technika tette lehetővé, hogy a repülőgép egy idegen területen szálljon le.

Egy másik világsajtót megjárt eset is bizonyította, hogy nem kell csúcstechnológiás katonai berendezés ehhez. 2013 júliusában a texasi Austin Egyetem tanára és hallgatói egy 80 millió dolláros yacht navigációs rendszerének spoofing technikával való meghamisításával térítették el egy kísérlet során a hajót és vezették más célponthoz. [17]

A módszer lényege az, hogy a megtámadott navigációs vevőkészülék helyén egy hamis jeladóból a valódi navigációs jelekkel mindenben megegyező struktúrájú jeleket sugároznak ki olyan teljesítménnyel, hogy azok a műholdakról származó valódi jeleket megfelelően elnyomják. A hamis jelekből meghatározható hely máshol van, mint a valóságos pillanatnyi helyzet, illetve az időt is megváltoztathatják. Terjedelmi okokból ennek a műszaki részleteivel és az ellene kidolgozott ún. anti-spoofing technikákkal egy későbbi cikkben foglalkozom.

ÖSSZEFOGLALÁS

A fenti, valóban csupán kiragadott példákból az elektronikai hadviselés egy vékony szeletébe kaphatott a Tisztelt Olvasó bepillantást. Ezeken kívül a navigációs rendszerek széles tárháza –

kezdve a rádió irányjel-adóktól a globális hiperbolikus navigációs rendszerekig – áll rendelkezésre, mind-mind sajátos elektronikai hadviselési megoldásokat követelve. Jelen írás azt mutatta be, hogy a leggyakrabban használt, legszélesebb körben ismert régi és új navigációs rendszerek milyen mértékben sérülékenyek, és ezek során mennyire sikerült az észrevétlen megtévesztést megvalósítani. A támadási módszerek tökéletesítésének fő célja az észrevétlen behatolás kell legyen a jövőben is.

FELHASZNÁLT IRODALOM

[1] MAGYAR HONVÉDSÉG ÖSSZHADERŐNEMI ELEKTRONIKAI HADVISELÉS DOKTRÍNA. 2. kiadás. MH DOFT kód: MD 3.6 (2) A MAGYAR HONVÉDSÉG KIADVÁNYA 2014. p. 16.

[2] DR. TAMÁSI FERENC: REH Rendszertechnika. Navigációs rendszerek. Zrínyi Miklós Katonai Akadémia Rádióelektronikai Tanszék, Budapest, 1978. pp.18-50.

[3] PIOTR KANIEWSKI: INS/TACAN/ALT - an alternative solution for positioning. http://mycoordinates.org/instacanalt-an-alternative-solution-for-positioning/all/1/ (2015. 03. 07.)

[4] SZ.N.: TACAN - Tactical Air Navigation. http://www.opticfox.com/2a4x2/tacan-fun.htm (2015. 03. 07.) Magyarra átdolgozta a szerző.

[5] SZ.N.: Tacan. http://www.pilotfriend.com/training/flight_training/nav/tacan.htm (2015. 03. 07.)

[6] SZ.N.: Electronics Technician Training and Reference Manuals. Tacan Equipment. http://electronicstechnician.tpub.com/14090/css/14090_35.htm (2015. 03. 07.) Átdolgozta a szerző.

[7] WWW.AIRFORCE.RU http://forums.airforce.ru/sovremennost/3950-reb-3/ (2015. 03. 07.)

[8] RUSSIAN GPS JAMMER http://www.qsl.net/n9zia/wireless/gps_jam-pics.html (2015. 03. 07.)

[9] SZ.N.: GPS JAMMER http://www.flickr.com/favicon.ico (2007. 12. 12.)

[10] DR. CARLO KOPP: Air Defence System Defensive Aids. http://www.ausairpower.net/APA-SAM-DefAids.html (2015. 03. 07.)

[11] CHINAJIAHO webáruház oldala. http://www.chinajiaho.com/adjustable-cell-phone-3g-and-gps-signal-jammer-with-four-bands-and-remote-control_p3410.html (2015. 03. 07.)

[12] GAJT ANTI-JAM ANTENNA http://www.novatel.com/products/gnss-antennas/gajt/#overview (2015. 03. 07.)

[13] GAJT BROCHURE http://www.amtechs.co.jp/2_gps/pdf/gajt-brochure.pdf (2015. 03. 07.)

[14] DAVID ROWE, JOHN WEGER, JOEL WALKER: Integrated GPS Anti-Jam Systems http://www.beidoudb.com:88/document/uploads/8bc7c219-713c-4cc0-8f38-a3f3df683082.pdf (2015. 03. 07.)

[15] GAJT - GPS-ANTI-JAM TECHNOLOGY http://www.forsbergservices.co.uk/products/antenna/gajt-gps-anti-jam-technology#noanchor (2015. 03. 07.)

[16] DR. HABIL. VÁNYA LÁSZLÓ: Kérdések és válaszok a szupertitkos RQ-170 iráni kézre kerüléséről. Repüléstudományi Közlemények XXVI. évfolyam 2013. 1. szám. pp. 634-641. HU ISSN 1789-770X http://www.repulestudomany.hu/kulonszamok/2012_cikkek/52_Vanya_Laszlo.pdf (2015. 03. 07.)

[17] SZ.N.: UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ (2015. 03. 07.)